



## DEPARTMENT OF AGRICULTURE

### Economic Research Service

#### Agency Information Collection Activities: Comment Request

**AGENCY:** Economic Research Service, US Department of Agriculture.

**ACTION:** Notice.

**SUMMARY:** Economic Research Service (ERS) within US Department of Agriculture (USDA) invites the general public and other Federal agencies to comment on a proposed information collection. ERS plans to collect information from the public to fulfill its data security requirements when providing access to restricted use microdata for the purpose of evidence building. ERS's data security agreements and other paperwork along with the corresponding security protocols allow ERS to maintain careful controls on confidentiality and privacy, as required by law. The purpose of this notice is to allow for 60 days of public comment on the proposed data security information collection, prior to submission of the information collection request (ICR) to the Office of Management and Budget (OMB).

**DATES:** Written comments on this notice must be received by **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** to be assured of consideration. Comments received after that date will be considered to the extent practicable. Send comments to the address below.

*Comments:* Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of ERS, including whether the information will have practical utility; (b) the accuracy of ERS's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information on respondents, including through the use of automated collection techniques or other forms of information technology; and (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic,

mechanical, or other technological collection techniques or other forms of information technology.

**ADDRESSES:** Address all comments concerning this notice to [ers.pra@usda.gov](mailto:ers.pra@usda.gov) identified by docket number 0535-NEW.

**FOR FURTHER INFORMATION CONTACT:** Requests for additional information or copies of this information collection should be directed to Julie Parker at [ers.pra@usda.gov](mailto:ers.pra@usda.gov) or 202-923-4910.

**SUPPLEMENTARY INFORMATION:** The Foundations for Evidence-Based Policymaking Act of 2018 mandates that the Office of Management and Budget (OMB) establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. While the adoption of the SAP is required for statistical agencies and units designated under CIPSEA, it is recognized that other agencies and organizational units within the Executive branch may benefit from the adoption of the SAP to accept applications for access to confidential data assets. The SAP is to be a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access confidential data assets held by a federal statistical agency or unit for the purposes of developing evidence. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP Project Management Office (PMO) and with OMB to implement the SAP. The SAP Portal is to be a single web-based common application for the public to request access to confidential data assets from federal statistical agencies and units. The National Center for Science and Engineering Statistics (NCSES), within the National Science Foundation (NSF), submitted a Federal Register Notice announcing plans to collect information through the SAP Portal (87 FR 53793).

Once an application for confidential data is approved through the SAP Portal, ERS will collect information to meet its data security requirements. This collection will occur outside of the SAP Portal.

*Title of collection:* Data Security Requirements for Accessing Confidential Data

*OMB Control Number:* 3145-NEW

*Expiration Date of Current Approval:* Not Applicable.

*Type of Request:* Intent to seek approval to collect information from the public to fulfill Economic Research Service's security requirements allowing individuals to access confidential data assets for the purposes of building evidence.

*Abstract:*

Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (hereafter referred to as the Evidence Act) mandates that OMB establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. Specifically, the Evidence Act requires OMB to establish a common application process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply for access to confidential data assets collected, accessed, or acquired by a statistical agency or unit. This new process will be implemented while maintaining stringent controls to protect confidentiality and privacy, as required by the law.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the local, State, Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, ERS is required by law to maintain careful controls that allow it to minimize disclosure risk while protecting confidentiality and privacy. The fulfillment of ERS data security requirements places a degree of burden on the public, which is outlined below.

The SAP Portal is a web-based application for the public to request access to confidential data assets from federal statistical agencies and units. The objective of the SAP Portal is to

increase public access to confidential data for the purposes of evidence building and reduce the burden of applying for confidential data. Once an individual's application in the SAP Portal has received a positive determination, the data-owning agency(ies) or unit(s) will begin the process of collecting information to fulfill their data security requirements.

The paragraphs below outline the SAP Policy, the steps to complete an application through the SAP Portal, and the process for agencies to collect information fulfilling their data security requirements.

### *The SAP Policy*

At the recommendation of the ICSP, the SAP Policy establishes the SAP to be implemented by statistical agencies and units and incorporates directives from the Evidence Act. The policy is intended to provide guidance as to the application and review processes using the SAP Portal, setting forth clear standards that enable statistical agencies and units to implement a common application form and a uniform review process. The SAP Policy was submitted to the public for comment in January 2022 (87 FR 2459, 2022). The policy is currently under review and has not yet been finalized.

### *The SAP Portal*

The SAP Portal is an application interface connecting applicants seeking data with a catalog of data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal will provide a streamlined application process across agencies, reducing redundancies in the application process. This single SAP Portal will improve the process for applicants, tracking and communicating the application process throughout its lifecycle. This reduces redundancies and burden on applicants that request access to data from multiple agencies. The SAP Portal will automate key tasks to save resources and time and will bring agencies into compliance with the Evidence Act statutory requirements.

## *Data Discovery*

Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP data catalog, maintained by federal statistical agencies at [www.researchdatagov.org](http://www.researchdatagov.org). Potential applicants can search by agency, topic, or keyword to identify data of interest or relevance. Once they have identified data of interest, applicants can view metadata outlining the title, description or abstract, scope and coverage, and detailed methodology related to a specific data asset to determine its relevance to their research.

While statistical agencies and units shall endeavor to include metadata in the SAP data catalog on all confidential data assets for which they accept applications, it may not be feasible to include metadata for some data assets (e.g., potential curated versions of administrative data). A statistical agency or unit may still accept an application through the SAP Policy even if the requested data asset is not listed in the SAP data catalog.

## *SAP Application Process*

Individuals who have identified and wish to access confidential data assets will be able to apply for access through the SAP Portal when it is released to the public in late 2022. Applicants must create an account and follow all steps to complete the application. Applicants begin by entering their personal, contact, and institutional information, as well as the personal, contact, and institutional information of all individuals on their research team. Applicants proceed to provide summary information about their proposed project, to include project title, duration, funding, timeline, and other details including the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP data catalog, including non-federal data sources. Applicants then proceed to enter detailed information regarding their proposed project, including a project abstract, research question(s), literature review, project scope, research methodology, project products, and anticipated output. Applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

### *Submission for Review*

Upon submission of their application, applicants will receive a notification that their application has been received and is under review by the data owning agency or agencies (in the event where data assets are requested from multiple agencies). At this point, applicants will also be notified that application approval does not alone grant access to confidential data, and that, if approved, applicants must comply with the data-owning agency's security requirements outside of the SAP Portal, which may include a background check.

In accordance with the Evidence Act and the direction of the ICSP, agencies will approve or reject an application within a prompt timeframe. In some cases, agencies may determine that additional clarity, information, or modification is needed and request the applicant to "revise and resubmit" their application. This is also in accordance with the SAP Policy, which was submitted to the public for comment in January 2022 (87 FR 2459, 2022). The policy is currently under review and has not yet been finalized.

Data discovery, the SAP application process, and the submission for review are planned to take place within the web-based SAP Portal. The notice announcing plans to collect information through the SAP Portal has been published separately (87 FR 53793).

### *Access to Restricted Use Data*

In the event of a positive determination, the applicant will be notified that their proposal has been accepted. The positive or final adverse determination concludes the SAP Portal process. In the instance of a positive determination, the data-owning agency (or agencies) will contact the applicant to provide instructions on the agency's security requirements that must be completed to gain access to the confidential data. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.

### *Collection of Information for Data Security Requirements*

In the instance of a positive determination for an application requesting access to a ERS confidential data asset, ERS will contact the applicant(s) to initiate the process of collecting

information to fulfill their security requirements. These include additional requirements necessary for the statistical agency or unit to place the applicant(s) in a trusted category that may include the applicant's successful completion of a background investigation, confidentiality training, nondisclosure, and data use agreements.

ERS's data security requirements include the collection of the following information:

- CIPSEA Training: ERS personnel provide a Security Briefing to all applicants who were approved access to restricted data. The Briefing includes information on the Confidential Information Protection and Statistical Efficiency Act of 2018, Title III of Pub. L. No. 115-435, codified in 44 U.S.C. Ch. 35 and other applicable Federal laws that protect the restricted data. Researchers will be asked to fill out the *CIPSEA Review Form* to verify that they reviewed the training.
- Completion of form *Certification and Restrictions on the Use of Confidential ERS Data*. This form is required to be signed by researchers who have been approved to access unpublished ERS data (alternatively, some approved researchers complete on-line training in lieu of completing this form). The form contains excerpts of the various laws that apply to the unpublished data being provided to the researcher. The form explains the restrictions associated with the unpublished data and includes a place for the research to sign the form, thereby acknowledging the restrictions and agreeing to abide by them.
- Completion of *ERS Data Remote Workplace Security Inspection Checklist*. Researchers approved to access unpublished ERS data do so using a secure data enclave environment accessible at their own location. An ERS employee performs a site inspection (either in-person or via a video call) of the researcher's location prior to the researcher being granted access to the unpublished data. During the site inspection, the ERS employee administers the form *ERS Site Inspection Checklist*, which asks questions pertaining to the suitability of the location for restricted data access and some of the policies associated

with accessing the restricted data. The form also collects information about the computer the researcher will use to access the ERS data enclave.

- Completion of *ERS Memorandum of Understanding (MOU)*. Researchers approved to access unpublished ERS data need to complete a Memorandum of Understanding Agreement between the Economic Research Service and their university, institution, or agency. The form establishes data access protocols and party responsibilities. If necessary, researchers may request an extension to their MOU using the *Extension of MOU Request Form*.
- If a researcher wishes to add a new researcher to their previously approved project, they can fill out the *Amendment for New Collaborators*. If a researcher wishes to change the scope of a previously approved project, they may fill out the *Request for Amended Project Agreement Form*.

*Estimate of Burden:* The amount of time to complete the agreements and other paperwork that comprise ERS's security requirements will vary based on the confidential data assets requested and the access modality. To obtain access to ERS confidential data assets, it is estimated that the average time to complete and submit ERS data security agreements and other paperwork is 110 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications occur prior to and separate from ERS effort to collect information related to data security requirements.

The expected number of applications in the SAP Portal that receive a positive determination from ERS in a given year may vary. Overall, per year, ERS estimates it will collect data security information for 120 application submissions that received a positive determination within the SAP Portal. ERS estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 1,080 hours and, as a result, an average annual burden of 360 hours.



**Spiro Stefanou,**

*Administrator, Economic Research Service,*

*United States Department of Agriculture.*

[FR Doc. 2022-27772 Filed: 12/22/2022 8:45 am; Publication Date: 12/23/2022]